

REMARKS

This Amendment is fully responsive to the final Office Action dated February 9, 2009, issued in connection with the above-identified application. A petition for a one-month extension of time accompanies this Amendment. Claims 35-62 were previously pending in the present application. With this Amendment, claims 36 and 54 have been canceled without prejudice or disclaimer to the subject matter therein; and claims 35, 37-41, 45-47, 52, 53, and 55-62 have been amended. Accordingly, claims 35, 37-53, and 55-62 are all the claims pending in the present application. No new matter has been introduced by the amendments made to the claims. Favorable reconsideration is respectfully requested.

In the Office Action, claims 59 and 60 have been objected to for minor informalities. Claims 59 and 60 have been amended herein to be consistent with the suggestions made by the Examiner. Withdrawal of the objection to claims 59 and 60 is now respectfully requested.

In the Office Action, claim 53 has been rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter. Specifically, the Examiner alleges that the Applicants' disclosure on page 24, line 31 to page 25, line 2 suggests that claim 53 is directed to an embodiment of the invention that is entirely software. As such, the claim lacks the necessary physical articles or objects to constitute a machine or manufacture within the meaning of 35 U.S.C. 101. Claims 54-59 have been rejected based merely on their dependencies from independent claim 53.

Claim 54 has been canceled thereby rendering the above rejection to that claim moot. Additionally, claim 53 has been rewritten as a software claim. The claim now recites "a computer-readable medium on which a program is stored...." Thus, claim 53 is now directed to a statutory software claim within the meaning of 35 U.S.C. 101 (see MPEP 2106.01). Withdrawal of the rejection to claims 53-59 under 35 U.S.C. 101 is now respectfully requested.

In the Office Action, claim 62 has been rejected under 35 U.S.C. 102(b) as being anticipated by Lotspiech (U.S. Patent No. 6,118,873, hereafter "Lotspiech"); and claims 35, 36, 40-42, 46-48, 52-54 and 58-61 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech. Claim 36 has been canceled thereby rendering the above rejection to that claim moot. Additionally, the Applicants have amended independent claims 35, 41, 47, 53 and 60-62

to help further distinguish the present invention from the cited prior art. For example, independent claim 35 (as amended) recites the following features:

“[a] copyright protection system comprising:

a recording apparatus configured to encrypt a content and to record the encrypted content;

a recording medium on which the encrypted content is recorded; and

a plurality of reproduction apparatuses, each of which is configured to read out and

decrypt the encrypted content recorded on said recording medium,

wherein each of said plurality of reproduction apparatuses is one of either a first plurality of reproduction apparatuses which belong to a first category and hold plural device keys in association with information regarding generations of the plural device keys or a second plurality of reproduction apparatuses which belong to a second category and hold only one device key, the plural device keys including a device key held since before and a device key provided in response to when revocation stops functioning,

said recording apparatus is configured (a) to generate, for said plurality of reproduction apparatuses and based on a media key and a device key held by each of said plurality of reproduction apparatuses, a plurality of revocation data intended for revoking a device key held by a specific reproduction apparatus of a respective category, (b) to generate the encrypted content which is the content encrypted based on the media key, and (c) to record the plurality of revocation data, information regarding a generation of the device key for generating each of the plurality of revocation data, and the encrypted content onto said recording medium,

the first plurality of reproduction apparatuses are each configured (a) to read out, from said recording medium, the plurality of revocation data corresponding to said first plurality of reproduction apparatuses, the information regarding the generations of the device key, and the encrypted content, and (b) to decrypt the encrypted content based on the plurality of revocation data read out and the information regarding the generation of the device key,

the second plurality of reproduction apparatuses are each configured (a) to read out, from said recording medium, the plurality of revocation data corresponding to said second plurality of reproduction apparatuses and the encrypted content, and (b) to decrypt the encrypted content

based on the plurality of revocation data read out,

each one of the plurality of revocation data is encrypted media key data which is the media key encrypted using a device key held by said plurality of reproduction apparatuses of a corresponding category.

the first plurality of reproduction apparatuses are each configured (a) to read out, from said recording medium, the corresponding encrypted media key data, the information regarding the generation of the device key, and the encrypted content, (b) to select a device key associated with the information regarding the generation of the device key, from among the held plural device keys (c) to obtain the media key by decrypting the encrypted media key data using the selected device key, and (d) to decrypt the encrypted content based on the obtained media key, and

the second plurality of reproduction apparatuses are each configured (a) to read out, from said recording medium, the corresponding encrypted media key data and the encrypted content, (b) to obtain the media key by decrypting the encrypted media key data using the held device key, and (c) to decrypt the encrypted content based on the obtained media key.” (Emphasis added).

The features emphasized above in independent claim 35 are similarly recited in independent claims 41, 47, 53 and 60-62. Specifically, claim 41 is directed to a recording apparatus, claim 47 is directed to a recording medium, claim 53 is directed to a computer-readable recording medium, claim 60 is directed to a copyright protection system, claim 61 is directed to a recording method, and claim 62 is directed to a reproduction method. Additionally, claims 41, 47, 53 and 60-62 have been amended in the same manner as claim 35.

Independent claims 35, 41, 47, 53 and 60-62 have been amended to incorporate the limitations of claim 36 and to clarify the relationship between the device key and the information regarding the generation of the device key (hereafter referred to as generation information). Thus, the features emphasized above in independent claim 35 (and similarly recited in independent claims 41, 47, 53 and 60-62) are fully supported by the Applicants’ disclosure.

The present invention (as similarly recited in independent claims 35, 41, 47, 53 and 60-62) is distinguishable over the cited prior art for at least the following reasons:

(a) Each of the first plurality of reproduction apparatuses (hereafter referred to as a first reproduction apparatus) holds a device key that is provided every time revocation has stopped functioning, in association with generation information. Specifically, the first reproduction apparatus holds pairs of corresponding device keys and generation information.

(b) The first reproduction apparatus selects, from among the plural device keys that it holds, a device key associated with the generation information read from the recording medium. Specifically, the first reproduction apparatus decrypts the encrypted media key data, using one and only one device key selected from among the plural device keys.

In the Office Action, the Examiner relies on Lotspeich for either anticipating or rendering obvious the features of independent claims 35, 41, 47, 53 and 60-62.

Specifically, in the final Office Action, the Examiner asserted that the user devices (video devices 18) disclosed in Lotspeich correspond to the first plurality of reproduction apparatuses in the present invention. Additionally, the Examiner raised the following points:

(a) The plural user devices disclosed in Lotspeich correspond to the reproduction apparatuses of the present invention (see Office Action page 6, last 2 lines) by referring to the description "[t]he system includes plural user devices, each of which includes plural computer-readable device keys selected from a set of device keys" in Lotspeich (see col. 1, line 66-col. 2, line 2). Furthermore, Lotspeich also discloses that "N device keys selected by a licensing agency are assigned to the video devices 18" (see col. 5, lines 42-44).

(b) The selected device key is "i" corresponds to the session key to be decrypted (see Office Action page 9, last 6 lines)" in Lotspeich by referring to the description "each session number can be represented by x_i . Each session number x_i is encrypted only by device keys in the i^{th} key dimension to render the session key block" in Lotspeich (see col. 2, lines 29-38). Lotspeich also discloses that "a decryption module that is accessible to each user device can access the device keys of the device to determine a session key based on the session key block and the respective device keys of the device" (see col. 2, lines 10-13).

However, the Applicants assert that the present invention (as recited in independent claims 35, 41, 47, 53 and 60-62, as amended) is clearly different from Lotspeich for at least the reasons

noted below.

First, the video device 18 disclosed in Lotspiech uses its device keys S₁₁ (i=1..., N) to decrypt the respective ith session numbers x_i (see col. 6, lines 34-37). Specifically, the video device 18 uses all the N device keys to decrypt the session key block and obtain the session key for decrypting a broadcast program.

On the other hand, the first reproduction apparatus in the present invention is different from the configuration in Lotspiech in terms of using one and only one device key selected from among plural device keys to decrypt revocation data and obtain a media key. The device keys in Lotspiech are one set consisting of N device keys, whereas the plural device keys in the present invention are independent of each other (i.e., never used at the same time).

Second, the video device 18 disclosed in Lotspiech updates the device keys using the session key and the Update Device Key Message 116 shown in Fig. 12 (see also col. 9, lines 3-5). Specifically, in this system, a compromised device key is updated (that is, overwritten) with a new device key for each of the video devices 18. Thus, in Lotspiech, the system encrypts a broadcast program and transmits the encrypted broadcast program, and each video device 18 is able to decrypt the broadcast program just by holding the newest device keys.

On the other hand, the first reproduction apparatus in the present invention must hold the device keys for the respective generations since content encrypted using an old device key is read from the recording medium. As such, the first reproduction apparatus in the present invention is different from that in Lotspiech in terms of holding a newly provided device key in addition to a device key held since before (that is, holding plural generations of device keys). Although Lotspiech discloses “the video devices can include a DVD player,” it does not disclose or suggest anything regarding above features or advantages of the present invention.

Finally, although the first reproduction apparatus in the present invention and the user device (video device 18) in Lotspiech have the common point of holding plural device keys, they are totally different in terms of the specific method of using the device keys (selecting and using one of the device keys as opposed to using all of the device keys) and the method of updating the device keys (holding plural device keys, one for each generation, as opposed to holding only the

newest keys).

Based on the above discussion, Lotspeich cannot anticipate or render obvious independent claims 35, 41, 47, 53 and 60-62 (as amended). Additionally, Lotspeich cannot anticipate or render obvious claims 40, 42, 46-48, 52, 58 and 59 at least by virtue of their respective dependencies from independent claims 35, 41, 47 and 53.

In the Office Action, claims 37, 43, 49 and 55 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspeich in view of Ishiguro (U.S. Publication No. 2001/044897, hereafter “Ishiguro”); and claims 38, 39, 44, 45, 50, 51, 56 and 57 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspeich in view of Masuda et al. (European Patent No. EP 09 69 667, hereafter “Masuda”).

Claims 37-39 depend from independent claim 35; claims 43-45 depend from independent claim 41; claims 49-51 depend from independent claim 47; and claims 55-57 depend from independent claim 53. As noted above, Lotspeich fails to anticipate or render obvious the features of independent claims 35, 41, 47 and 53 (as amended). Additionally, Ishiguro and Masuda fail to overcome the deficiencies noted above in Lotspeich. Accordingly, no combination of Lotspeich, Ishiguro and Masuda would result in, or otherwise render obvious, claims 37-39, 43-45, 49-51 and 55-57 at least by virtue of their respective dependencies from independent claims 35, 41, 47 and 53.

In light of the above, the Applicants respectfully submit that all the pending claims are patentable over the prior art of record. The Applicants respectfully request that the Examiner withdraw the rejections presented in the outstanding Office Action, and pass the present application to issue.

The Examiner is invited to contact the undersigned attorney by telephone to resolve any remaining issues.

Respectfully submitted,

Naoki YAMAMOTO et al.

/Mark D. Pratt/

By:2009.06.03 15:58:15 -04'00'

Mark D. Pratt
Registration No. 45794
Attorney for Applicants

MDP/ats
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
June 3, 2009